(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－110549
（P2003－110549A）
(43)公開日　平成15年４月11日(2003.4.11)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｈ　1/00	Ｆ	５Ｃ０６４
Ｈ０４Ｈ　1/00		Ｈ０４Ｎ　7/16	Ｚ	５Ｊ１０４
Ｈ０４Ｎ　7/16		Ｈ０４Ｌ　9/00　６４１		

審査請求　未請求　請求項の数10　書面　（全 13 頁）

(21)出願番号　特願2001－338753(P2001－338753)

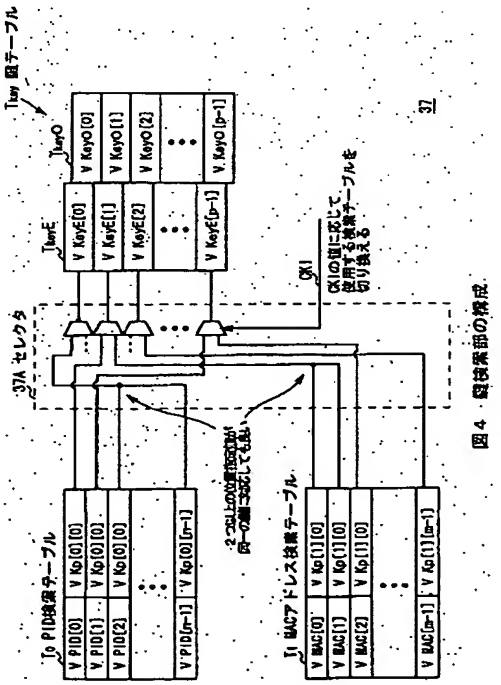
(22)出願日　平成13年９月28日(2001.9.28)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　赤地　正光
東京都品川区北品川６丁目７番35号ソニー株式会社内
(74)代理人　100082740
弁理士　田辺　恵基

Ｆターム(参考)　5C064 BA01 BB02 BC06 BC17 BC18
BC22 BC23 BD02 BD08 BD09
BD13
5J104 AA16 EA04 EA16 NA02 PA05

(54)【発明の名称】　情報伝送システム、受信装置、暗号鍵検索装置及び暗号鍵検索方法

(57)【要約】
【課題】簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システムを実現する。
【解決手段】複数の暗号鍵の中から選択した暗号鍵を用いてデータを暗号化して暗号化データを生成し、当該選択した暗号鍵に対応する検索キーを当該暗号化データに付して送信する送信装置と、複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する鍵検索手段と、当該取得した暗号鍵を用いて暗号化データを復号する復号手段とを有する受信装置を、情報伝送システムに用いる。



【特許請求の範囲】
【請求項１】複数の暗号鍵の中から選択した暗号鍵を用いてデータを暗号化して暗号化データを生成し、当該選択した暗号鍵に対応する検索キーを当該暗号化データに付して送信する送信装置と、
上記暗号化データを受信する受信手段と、上記複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する鍵検索手段と、上記取得した暗号鍵を用いて上記暗号化データを復号する復号手段とを有する受信装置とを具えることを特徴とする情報伝送システム。
【請求項２】複数の暗号鍵の中から選択された暗号鍵を用いて暗号化された暗号化データを受信する受信手段と、
上記複数の暗号鍵を記憶した鍵テーブルと、
複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、
上記暗号化データとともに送信される上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する暗号鍵検索手段と、
上記取得した暗号鍵を用いて上記暗号化データを復号する復号手段とを具えることを特徴とする受信装置。
【請求項３】上記暗号鍵検索手段は、上記暗号化データとともに送信される検索テーブル指定情報に基づいて複数個の上記検索テーブルから１つの検索テーブルを選択し、上記検索キーを用いて当該選択した検索テーブルを検索することを特徴とする請求項２に記載の受信装置。
【請求項４】上記暗号鍵検索手段は、上記暗号化データとともに送信される鍵テーブル指定情報に基づいて複数個の上記鍵テーブルから１つの鍵テーブルを選択し、上記検索キーに対応する暗号鍵を当該選択した鍵テーブルから取得することを特徴とする請求項２に記載の受信装置。
【請求項５】複数の暗号鍵を記憶した鍵テーブルと、
複数の検索キーと上記鍵テーブルにおける上記複数の暗号鍵との対応関係を記憶した検索テーブルと、
任意の上記検索キーを用いて上記検索テーブルを検索することにより、当該検索キーに対応する暗号鍵を上記鍵テーブルから取得する暗号鍵検索手段とを具えることを特徴とする暗号鍵検索装置。
【請求項６】上記暗号鍵検索手段は、所定の検索テーブル指定情報に基づいて複数個の上記検索テーブルから１つの検索テーブルを選択し、上記検索キーを用いて当該選択した検索テーブルを検索することを特徴とする請求項５に記載の暗号鍵検索装置。
【請求項７】上記暗号鍵検索手段は、所定の鍵テーブル指定情報に基づいて複数個の上記鍵テーブルから１つの鍵テーブルを選択し、上記検索キーに対応する暗号鍵を当該選択した鍵テーブルから取得することを特徴とする請求項５に記載の暗号鍵検索装置。
【請求項８】複数の検索キーと鍵テーブルが記憶する複数の暗号鍵との対応関係を記憶した検索テーブルを、任意の上記検索キーを用いて検索し、当該検索キーに対応する上記暗号鍵を上記鍵テーブルから取得することを特徴とする暗号鍵検索方法。
【請求項９】所定の検索テーブル指定情報に基づいて複数個の上記検索テーブルから１つの検索テーブルを選択し、上記検索キーを用いて当該選択した検索テーブルを検索することを特徴とする請求項８に記載の暗号鍵検索方法。
【請求項１０】所定の鍵テーブル指定情報に基づいて複数個の上記鍵テーブルから１つの鍵テーブルを選択し、上記検索キーに対応する暗号鍵を当該選択した鍵テーブルから取得することを特徴とする請求項８に記載の暗号鍵検索方法。
【発明の詳細な説明】
【００００】
【発明の属する技術分野】本発明は情報伝送システム、受信装置、暗号鍵検索装置及び暗号鍵検索方法に関し、例えばデータを暗号化し衛星を介して伝送する情報伝送システムに適用して好適なものである。
【００００】
【従来の技術】従来ディジタル衛星放送システムにおいて、受信契約を行った正当な受信者のみが放送を受信し得る限定受信機構（ＣＡ：Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ）が用いられている。
【００００】一般に限定受信機構においては、主に処理速度の問題から、送信側と受信側とで共通の暗号鍵を設定し、当該暗号鍵を用いて配信するデータストリームの暗号化及び復号化を行う共通鍵暗号化方式が適用されている。
【００００】かかる限定受信機構においては、受信契約を行った受信者に対して予め所定の暗号鍵を渡しておく。送信側はこの暗号鍵を用いて放送データを暗号化し、放送衛星を介して送信する。そして受信者は暗号鍵を用いて受信データの暗号化を解除することにより、受信契約を行った受信者のみが放送を視聴し得るようになされている。
【００００】暗号鍵は受信装置内部の記憶装置に記録されており、送信装置からの指示（例えば鍵の切り換えを指示する信号の送出や、暗号鍵の索引を特定し得るキーワードのデータストリームへの書き込み）に応じて、検索テーブル等の検索機構を用いて鍵を検索する。
【００００】ここで近年、ディジタル衛星放送システムを用いてデータ伝送を行う衛星データ伝送システムが実用化されている。衛星回線は電話回線やＩＳＤＮ回線等

に比べてその通信速度が速いため、大容量データを短時間で伝送することができという利点がある。

【００００】このような衛星データ伝送システムにおいて各受信者に対して個別のデータを伝送すると（これをユニキャスト通信と呼ぶ）、回線の利用効率が悪化してしまうという問題がある。このため衛星データ伝送システムにおいて、例えば受信者の属性等の適当な条件で複数の受信装置をグループ化し、同一のグループに属する受信装置に対して同報通信を行うことにより回線の利用効率を向上させる方法が考えられている。このようなグループに対する同報通信をマルチキャスト通信と呼ぶ。衛星データ伝送システムは本質的に同報性を有しているため、同報通信は容易に実現することができる。

【００００】個別通信と同報通信とでは受信装置におけるデータの処理方法が異なるため、鍵の索引となる識別符号の構成も異なる場合が多い。このため受信装置においては、どちらの通信方式でデータストリームが送信されているかを識別し、通信方式に応じた検索テーブルによって暗号鍵を検索する必要がある。

【００００】ここで、個別通信及び同報通信の両方に対応した受信装置においては、当該受信装置固有の個別鍵に加えて、所属するグループに割り当てられた共通鍵を持つ。そしてこの共通鍵はグループ毎に割り当てられているため、受信装置が複数のグループに所属している場合、所属するグループ全てについての共通鍵を持つ必要がある。

【００００】このため、このような個別通信及び同報通信の両方に対応した受信装置においては、個別鍵の検索テーブルと共通鍵の検索テーブルを持つことになり、構成が複雑になる、ひいては必要となる回路量も増大するという問題があった。

【００００】本発明は以上の点を考慮してなされたもので、簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システム、受信装置、暗号鍵検索装置及び暗号鍵検索方法を提案しようとするものである。

【００００】

【課題を解決するための手段】かかる課題を解決するため本発明においては、複数の暗号鍵の中から選択した暗号鍵を用いてデータを暗号化して暗号化データを生成し、当該選択した暗号鍵に対応する検索キーと当該検索キーの属する検索テーブルを選択する信号とを当該暗号化データに付して送信する送信装置と、暗号化データを受信する受信手段と、複数の暗号鍵を記憶した鍵テーブルと、複数の検索キー及び前記暗号鍵との対応関係を記憶した検索テーブルと、検索キーを用いて検索テーブルを検索することにより当該検索キーに対応する暗号鍵を鍵テーブルから取得する鍵検索手段と、当該取得した暗号鍵を用いて暗号化データを復号する復号手段とを有する受信装置とを備えるようにした。

【００００】複数の暗号鍵を記憶した選択可能な鍵テーブルと、複数の検索キーと鍵テーブルにおける複数の暗号鍵との対応関係を記憶した検索テーブルとを設け、当該検索テーブルを検索キーで検索して鍵テーブルから暗号鍵を取得するようにしたことにより、簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システムを実現できる。

【００００】

【発明の実施の形態】以下図面について本発明の一実施の形態を詳述する。

【００００】（１）衛星データ伝送システムの全体構成図１において、１は全体として本発明を適用した衛星データ伝送システムを示し、送信側システム２、衛星３、及び複数の同一構成でなる受信側システム４で構成される。送信側システム２と各受信側システム４とはそれぞれインターネット５を介して接続されている。また送信側システム２を管理するサービスプロバイダと各受信側システム４を所有する受信者との間では、予め当該衛星データ伝送システム１についての利用契約が結ばれている。

【００００】送信側システム２においては、当該送信側システム２全体を制御する制御装置１０、回線接続装置１１、データサーバ１２及び送信処理装置１３がローカルネットワーク１４を介して接続されている。

【００００】制御装置１０は、受信側システム４からインターネット５を介して送信されたデータ読出要求を回線接続装置１１を介して受信する。そして制御装置１０はデータ読出要求に応じて、データサーバ１２或いはインターネット５上のデータサーバ（図示せず）からデータを読み出し、送信処理装置１３に供給する。

【００００】送信処理装置１３は、供給されたデータをＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケット化した後暗号化し、さらに当該ＩＰパケットを、ＤＶＢ（ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇ）データ放送仕様（ＥＮ３０１　１９２）に準拠したセクションと呼ばれるデータブロックのペイロードに配置する。そして送信処理装置１３はセクションをＭＰＥＧ（ＭｏｖｉｎｇＰｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）２方式に準拠した所定長のパケットに分割した後、各パケットにＴＳパケットヘッダを付することによりＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケットを生成する。

【００００】ここで衛星データ伝送システム１においては、宛て先を識別する符号としてＭＰＥＧ２－ＴＳ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ２　Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）で規定するＰＩＤ（ＰａｃｋｅｔＩＤ）や、受信側装置４の受信装置２１や情報処理装置２２の固有の識別番号として用いているＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ：メディアアクセス制御）アドレスを利用している。そして送信処理装置１３は、衛星データ伝送システ

ム１で用いられる全ての暗号鍵を記述した鍵テーブルＴｋｅｙ、各グループのＰＩＤと鍵テーブルＴｋｅｙに記憶された暗号鍵との対応関係を記述したＰＩＤ検索テーブルＴ０、及び各受信装置２１及び情報処理装置２２それぞれのＭＡＣアドレスと鍵テーブルＴｋｅｙに記憶された暗号鍵との対応関係を記述したＭＡＣアドレス検索テーブルＴ１を有している。

【００００】制御装置１０はＰＩＤを用いて同報通信を行う場合はＰＩＤ検索テーブルＴ０の使用を、ＭＡＣアドレスを用いた個別通信の場合はＭＡＣアドレス検索テーブルＴ１の使用を送信処理装置１３に指定する。送信処理装置１３は指定された検索テーブルＴ０又はＴ１を用いてデータの送信先に応じた暗号鍵を検索し、当該検索した暗号鍵を用いて当該データを暗号化する。

【００００】このとき送信処理装置１３は、各セクションに付せられたヘッダ（セクションヘッダ）内のＣＫＩ（Ｃｏｍｍｏｎ　Ｋｅｙ　Ｉｎｄｉｃａｔｏｒ、後述）の値を、例えば同報通信でＰＩＤ検索テーブルＴ０を使用した場合は「０」、個別通信でＭＡＣアドレス検索テーブルＴ１を使用した場合は「１」とする。また送信処理装置１３は、同報通信の場合、送信先グループに対応したＰＩＤをＴＳパケットに付するのに対し、個別通信の場合、送信先装置のＭＡＣアドレスをセクションヘッダに記入する。

【００００】そして送信処理装置１３は、かくして生成したＴＳパケットからトランスポートストリームを生成し、さらに変調、増幅等の処理を施して、送信アンテナ１５を介してアップリンク波Ｓ２として衛星３に向けて送信する。

【００００】衛星３はアップリンク波Ｓ２を受信して増幅し、ダウンリンク波Ｓ３として地上の受信側システム４に向けて再送信する。

【００００】一方受信側システム４においては、受信装置２１、回線接続装置２３、及び、例えばパーソナルコンピュータ等でなる複数の情報処理装置２２が、ローカルネットワーク２４を介して相互に接続されている。

【００００】受信装置２１は、受信アンテナ２０を介して受信したダウンリンク波Ｓ３に対して復調処理及び後述する復号処理を行うことにより、ローカルネットワーク２４内の装置向けに送信されたデータを復号し、受信装置２１に内蔵した記憶装置、ないしはローカルネットワーク２４を介して情報処理装置２２に供給する。

【００００】また情報処理装置２２は、ユーザによってデータの読出要求操作が入力されると、これに応じてデータの読出要求を回線接続装置２３及びインターネット５を介して送信側システム２に送信する。

【００００】（２）受信装置の構成

次に、受信側システム４の受信装置２１を図２を用いて説明する。

【００００】受信装置２１においては、当該受信装置２１全体を制御するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｓｓｅｃｉｎｇ　Ｕｎｉｔ）３０に、バス３９を介してフロントエンド部３１、デマルチプレクサ３２、受信フィルタ３３、復号部３４、チェッカ３５、バッファ３６、鍵検索装置３７及びインターフェース部３８が接続されている。

【００００】フロントエンド部３１は、受信アンテナ２０を介して受信したダウンリンク波Ｓ３を復調し、トランスポートストリームＤ３１としてデマルチプレクサ３２に供給する。デマルチプレクサ３２はトランスポートストリームＤ３１からＰＩＤに基づいて必要なＴＳパケットのみを分離し、受信フィルタ３３に供給する。必要ならば受信フィルタ３３は、ＴＳパケットのヘッダ内容に基づいてデータ復号処理に不要なＴＳパケットを更に破棄し、残りのＴＳパケットを復号部３４に供給する。

【００００】復号部３４は後述する復号処理に基づいて動作し、これによって得られた検索情報をもって鍵検索装置３７に問い合わせを行い、当該鍵検索装置３７から暗号鍵を取得する。そして復号部３４は、ＴＳパケットを再構成してセクションを復元した後、鍵検索装置３７から取得した暗号鍵を用いて当該セクションのペイロードを復号することにより、ＩＰパケットでなる復号データストリームＤ３４を得る。

【００００】必要ならば復号部３４はチェッカ３５に復号データストリームＤ３４を供給し、正常に復号処理が行われたか否かを検定させる。これは例えば、送信側システム２から受信側システム４への暗号鍵の受け渡しが正常に行われなかったなどの理由により、誤った暗号鍵によって復号処理が行われた場合を想定しており、例えば送信処理装置１３に入力するデータ列に対してＣＲＣ（Ｃｙｃｒｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｏｄｅ）等の検査符号を付加した上で暗号化処理を行い、チェッカ３５は復号データストリームＤ３４において算出されたＣＲＣの値が復号されたＣＲＣの値と合致することによって処理が正常に完了したと判定する。なお、このチェッカ３５の動作は付加機能であり、その存在の有無は本発明の効果には影響しない。そしてチェッカ３５の処理を行わないのであれば、復号部３４は復号データストリームＤ３４をバッファ３６に直接供給する。

【００００】上述したフロントエンド部３１からチェッカ３５に至るまでの処理はＣＰＵ３０の処理とは独立して行われ、このためチェッカ３５が復号データストリームＤ３４を出力可能な瞬間に、ＣＰＵ３０が当該復号データストリームＤ３４を処理可能であるとは限らない。このタイムラグを調整するため、バッファ３６は復号データストリームＤ３４を一時的に蓄積する。バッファ３６に蓄積された復号データストリームＤ３４は、ＣＰＵ３０の制御に応じて読み出されインターフェイス部３８に入力され、ローカルネットワーク２４（図１）を介して情報処理装置２２に供給される。

【００００】（３）受信装置における復号処理
上述したようにセクションにおいては、ペイロードの先頭にセクションヘッダが付加されている。ＤＶＢデータ放送仕様（ＥＮ　３０１　１９２）によれば、セクションヘッダのビットの割り付けは図３に示す通りであり、各データバイトは走査線順に送信される。ここでＭＡＣアドレス＃６とは、ＭＡＣアドレスの最上位ビットをＢｉｔ４７、最下位ビットをＢｉｔ０としたときの、Ｂｉｔ７からＢｉｔ０を含むバイト（８ｂｉｔ）を意味する。
【００００】本発明による衛星データ伝送システム１においては、特開２００１－１３６１５９で示された衛星データ伝送システムと同様に、セクションヘッダ６バイト目の最上位ビット（図３の２行めの第２番目のバイトのＤ７）をＣＫＩと定める。そして衛星データ伝送システム１においては、上述したようにＣＫＩの値を、同報通信でＰＩＤ検索テーブルＴ０を使用した場合は「０」、個別通信でＭＡＣアドレス検索テーブルＴ１を使用した場合は「１」とする。
【００００】ここで、ＤＶＢデータ放送仕様においては、ＣＫＩは「Ｒｅｓｅｒｖｅｄ」とされており、値として「１」をとるように定められている。ＰＩＤを用いた同報通信はＭＡＣアドレスを用いた個別通信に比べてより特殊な処理方法であると考えられるので、同報通信のときにＣＫＩを「０」とすると定めることで、ＤＶＢデータ放送仕様との仕様を一致することができる。さらに、特開２００１－１３６１５９で示された衛星データ伝送システムにおいては、本願発明と同様に同報通信で共通鍵を使用した場合にＣＫＩを「０」とし、個別通信で個別鍵を使用した場合にＣＫＩを「１」とするようになされており、このため特開２００１－１３６１５９で示された衛星データ伝送システムを容易に拡張して本願発明に適用することができる。
【００００】受信装置２１の復号部３４は、セクションヘッダのＣＫＩの値に基づいて通信方式を判別する。そして復号部３４は鍵検索部３７に対して問い合わせを行い、ＣＫＩが「０」で同報通信の場合、ＴＳパケットのＰＩＤを検索キーとしてこれに対応する暗号鍵をＰＩＤ検索テーブルＴ０から検索し、ＣＫＩが「１」で個別通信の場合、セクションヘッダのＭＡＣアドレスを検索キーとしてこれに対応する暗号鍵をＭＡＣアドレス検索テーブルＴ１を用いて検索する。
【００００】図４は鍵検索部３７の構成を示し、上述したＰＩＤ検索テーブルＴ０、ＭＡＣアドレス検索テーブルＴ１及び鍵テーブルＴｋｅｙを有しているとともに、当該検索テーブルＴ０又はＴ１の一方を選択するセレクタ３７Ａを有している。
【００００】鍵テーブルＴｋｅｙはｐ個のレコードを有しており、各レコードには暗号鍵が記録されている。ここで実際上衛星データ伝送システム１においては、Ｅｖｅｎ期間とＯｄｄ期間の２つの暗号鍵系列を有しており、これらをセクションヘッダの特定のビットに従って切り換えて使用することにより、暗号鍵の更新等を高速に実行し得るようになされている。このため鍵テーブルＴｋｅｙは、Ｅｖｅｎ期間の暗号鍵（「ＫｅｙＥ」で示す）を格納した鍵テーブルＴｋｅｙＥと、Ｏｄｄ期間の暗号鍵（「ＫｅｙＯ」で示す）を格納した鍵テーブルＴｋｅｙＯとで構成される。このような仕組みについても本発明は問題なく適用できる。
【００００】また、ＰＩＤ検索テーブルＴ０においてはｎ個のレコードを有しており、それぞれに検索キーとしてのＰＩＤの値と、鍵テーブルＴｋｅｙ内における当該ＰＩＤに対応した暗号鍵の位置（例えばレコード番号）を示す位置指定値Ｋｐが記録されている。同様にＭＡＣアドレス検索テーブルＴ１においてはｍ個のレコードを有しており、それぞれに検索キーとしてのＭＡＣアドレスの値と、鍵テーブルＴｋｅｙ内における当該ＭＡＣアドレスに対応した暗号鍵の位置を示す位置指定値Ｋｐとが記録されている。なお、Ｋｐ［ｘ］［ｙ］は、テーブルｘの第ｙ行目のレコードを示すものである。
【００００】ここで検索テーブルＴ０及びＴ１においては、異なる検索キーに対して同一値の位置指定値Ｋｐが対応付けられていてもかまわない。例えば、複数のＭＡＣアドレスに対して同一の暗号鍵を割り当てる場合、これらのＭＡＣアドレスに対する位置指定値Ｋｐは同一値となる。
【００００】なお、鍵テーブルＴｋｅｙ内の各暗号鍵、ＰＩＤ検索テーブルＴ０内の各ＰＩＤ及び各位置指定値Ｋｐ、並びにＭＡＣアドレス検索テーブルＴ１内の各ＭＡＣアドレス及び各位置指定値Ｋｐには、それぞれ有効／無効を表すＶａｌｉｄビット（「Ｖ」で示す）が設けられており、それぞれの有効／無効を独立して設定し得るようになされている。なおＶａｌｉｄビットは、その値が「１」の時有効とし、「０」の時無効とする。また、Ｅｖｅｎ期間の鍵テーブルＴｋｅｙＥを用いて暗号化した場合、後述するＰＳＣ（Ｐａｙｌｏａｄ　ＳｃｒａｍｂｌｉｎｇＣｏｎｔｒｏｌ）の上位ビットの値を「０」とし、Ｏｄｄ期間の鍵テーブルＴｋｅｙＯを用いて暗号化した場合、ＰＳＣの上位ビットの値を「１」とする。
【００００】このように鍵検索部３７は、暗号鍵の実体を記憶した鍵テーブルＴｋｅｙと、当該鍵テーブルＴｋｅｙ内の各暗号鍵と検索キー（ＰＩＤ又はＭＡＣアドレス）との対応関係を記述したＰＩＤ検索テーブルＴ０及びＭＡＣアドレス検索テーブルＴ１とを有している。このため鍵検索部３７は、ＰＩＤ検索テーブル及びＭＡＣアドレス検索テーブルそれぞれに鍵フィールドを設ける場合に比べ、鍵検索部３７の回路規模を削減することができる。
【００００】鍵検索部３７のセレクタ３７Ａは、ＣＫＩ

が「０」のときＰＩＤ検索テーブルＴ０を選択する。そして鍵検索部３７はＴＳパケットのＰＩＤを検索キーとしてＰＩＤ検索テーブルＴ０を検索し、ＰＩＤの値が合致するレコードに記録された位置指定値Ｋｐが示す暗号鍵を鍵テーブルＴｋｅｙから読み出して復号部３４に供給する。また鍵検索部３７のセレクタ３７Ａは、ＣＫＩが「１」のときＭＡＣアドレス検索テーブルＴ１を選択する。そして鍵検索部３７はセクションヘッダのＭＡＣアドレスを検索キーとしてＭＡＣアドレス検索テーブルＴ１を検索し、ＭＡＣアドレスの値が合致するレコードに記録された位置指定子Ｋｐが示す暗号鍵を鍵テーブルＴｋｅｙから読み出して復号部３４に供給する。

【００００】そして復号部３４は、かくして得た暗号鍵を用い、セクションのペイロードに配置されたＩＰパケットを復号する。

【００００】（４）復号処理手順

次に、受信装置２１における復号処理手順を図５のフローチャートを用いて説明する。

【００００】復号部３４はＲＴ１で処理を開始し、ステップＳＰ１において、セクションヘッダに記述されているＭＡＣアドレスをレジスタＭＲに代入するとともに、ＴＳパケットのＰＩＤをレジスタＰＲに代入し、次のステップＳＰ２に進む。

【００００】ステップＳＰ２において復号部３４は、セクションヘッダにおけるＰＳＣ（Ｐａｙｌｏａｄ　Ｓｃｒａｍｂｌｉｎｇ　Ｃｏｎｔｒｏｌ）（図３）の下位ビットの値を参照し、当該セクションのペイロードのデータ（すなわちＩＰパケット）が暗号化されているか否かを判断する。ステップＳＰ２において否定結果が得られた場合、このことは下位ビットが「０」であり、当該セクションのペイロードに配置されたＩＰパケットが暗号化されていないことを表しており、復号部３４はステップＳＰ１２へ進み、暗号解除処理を行わずにセクションを後段のチェッカ３５に送出し処理を終了する。

【００００】これに対してステップＳＰ２において肯定結果が得られた場合、このことはＰＳＣの下位ビットが「１」であり、当該セクションのペイロードに配置されたＩＰパケットが暗号化されていることを表しており、復号部３４はステップＳＰ３に進む。

【００００】ステップＳＰ３において復号部３４は、セクションヘッダにおけるＣＫＩ（図３）の値に基づいて、ＰＩＤ検索テーブルＴ０を用いて暗号鍵を検索すべきか、ＭＡＣアドレス検索テーブルＴ１を用いて暗号鍵を検索すべきかを判断する。ステップＳＰ３において肯定結果が得られた場合、このことはＣＫＩが「０」であり、当該セクションが同報通信のセクションで、ＰＩＤ検索テーブルＴ０を用いて暗号鍵を検索すべきことを表しており、復号部３４はステップＳＰ４へ進む。

【００００】ステップＳＰ４において、復号部３４は鍵検索部３７に対して問い合わせを行い、レジスタＰＲに記憶されているＰＩＤの値を検索キーとしてＰＩＤ検索テーブルＴ０を検索する。鍵検索部３７におけるＰＩＤ検索テーブルＴ０の検索は、当該ＰＩＤ検索テーブルＴ０の先頭レコードから順に、ＰＩＤフィールド及び位置指定値フィールド双方が有効（すなわち双方のＶａｌｉｄビットがともに「１」）なレコードに対してＰＩＤが合致するまで行われる。

【００００】そして復号部３４は、ＰＩＤ検索テーブルＴ０内にＰＩＤが合致するレコードが存在しなかった場合、ステップＳＰ１１に移って当該セクションを破棄した後、ステップＳＰ１２に移って当該セクションに対する処理を終了する。

【００００】これに対して復号部３４は、ＰＩＤ検索テーブルＴ０内にＰＩＤが合致するレコードが存在した場合、ステップＳＰ５に移って当該合致したレコードの位置指定値Ｋｐ［０］［ｙ］をレジスタＫｐに代入し、ステップＳＰ８に移る。

【００００】一方、ステップＳＰ３において否定結果が得られた場合、このことはＣＫＩが「１」であり、当該セクションが個別通信のセクションで、ＭＡＣアドレス検索テーブルＴ１を用いて暗号鍵を検索すべきことを表しており、復号部３４はステップＳＰ６へ進む。

【００００】ステップＳＰ６において復号部３４は鍵検索部３７に問い合わせを行い、レジスタＭＲに記憶されているＭＡＣアドレスの値を検索キーとしてＭＡＣアドレス検索テーブルＴ１を検索する。鍵検索部３７におけるＭＡＣアドレス検索テーブルＴ１の検索はステップＳＰ４と同様に、当該ＭＡＣアドレス検索テーブルＴ１の先頭レコードから順に、ＭＡＣアドレスフィールド及び位置指定値フィールド双方が有効なレコードに対してＭＡＣアドレスが合致するまで行われる。

【００００】そして復号部３４は、ＭＡＣアドレス検索テーブルＴ１内にＭＡＣアドレスが合致するレコードが存在しなかった場合、ステップＳＰ１１に移って当該セクションを破棄した後、ステップＳＰ１２に移って当該セクションに対する処理を終了する。

【００００】これに対して復号部３４は、ＭＡＣアドレス検索テーブルＴ１内にＭＡＣアドレスが合致するレコードが存在した場合、ステップＳＰ７に移って当該合致したレコードの位置指定値Ｋｐ［１］［ｙ］をレジスタＫｐに代入し、ステップＳＰ８に移る。

【００００】ステップＳＰ８において復号部３４は、ＰＳＣの上位ビットをレジスタＥＯに代入する。そして復号部３４は、レジスタＥＯの値が「０」のとき、Ｅｖｅｎ期間の鍵テーブルＴｋｅｙＥから、レジスタＫｐの値に対応するＥｖｅｎ期間の鍵ＫｅｙＥ［Ｋｐ］についてのＶａｌｉｄビットをレジスタＶａｌｉｄに代入するのに対し、レジスタＥＯの値が「１」のとき、Ｏｄｄ期間の鍵テーブルＴｋｅｙＯから、レジスタＫｐの値に対応するＯｄｄ期間の鍵ＫｅｙＯ［Ｋｐ］についてのＶａｌ

ｉｄビットをレジスタＶａｌｉｄに代入し、次のステップＳＰ９に移る。

【０００９】ステップＳＰ９において復号部３４は、レジスタＶａｌｉｄの値に基づいて、暗号鍵の有効／無効を判断する。ステップＳＰ９において否定結果が得られた場合、このことはＰＩＤ又はＭＡＣアドレスに対応する暗号鍵が存在するにもかかわらず、当該暗号鍵が無効状態にあることを表しており、復号部３４はステップＳＰ１１に移って当該セクションを破棄した後、ステップＳＰ１２に移って当該セクションに対する処理を終了する。

【０００９】これに対してステップＳＰ９において肯定結果が得られた場合、このことはＰＩＤ又はＭＡＣアドレスに対応する暗号鍵が存在し、なおかつ当該暗号鍵が有効状態にあることを表しており、復号部３４は次のステップＳＰ１０に移る。

【０００９】ステップＳＰ１０において復号部３４は、鍵テーブルＴｋｅｙからレジスタＫｐ及びレジスタＥＯに対応する鍵データＫｅｙ［Ｋｐ，ＥＯ］を取り出し、当該鍵データを用いてセクションのペイロードを復号し、ステップＳＰ１２に移って処理を終了する。

【０００９】かくして復号部は、２つの異なる鍵検索方式に対応した復号処理を行う。

【０００９】（５）動作及び効果

以上の構成において、送信側システム２の送信処理装置１３は、受信側システム４のデータ読み出し要求に応じたデータをデータサーバから読み出し、これをＩＰパケット化した後、さらに暗号化、セクション化及びＴＳパケット化し、アップリンク波Ｓ２として送信アンテナ１５を介して衛星３に送信する。

【０００９】このとき送信処理装置１３は、送信するデータの通信形式が同報通信の場合、送信先グループに割り当てられたＰＩＤに対応する暗号鍵をＰＩＤ検索テーブルＴ０を用いて検索し、これにより得られた暗号鍵を用いて暗号化するとともに、当該ＰＩＤをＴＳパケットに記入し、さらにセクションヘッダ内のＣＫＩの値を「０」とする。

【０００９】これに対して送信処理装置１３は個別通信の場合、送信先装置に割り当てられたＭＡＣアドレスに対応する暗号鍵をＭＡＣアドレス検索テーブルＴ１を用いて検索し、これにより得られた暗号鍵を用いて暗号化するとともに、当該ＭＡＣアドレスをセクションヘッダに記入し、さらにＣＫＩの値を「１」とする。

【０００９】受信側システム４の受信装置２１は、受信アンテナ３９を介して受信したダウンリンク波Ｓ３を復調してトランスポートストリームＤ３１を生成する。受信装置２１の復号部３４は、トランスポートストリームＤ３１内のＴＳパケットからセクションを再構成する。

【０００９】そして復号部３４は、鍵検索部３７に問い合わせを行い、セクションヘッダのＣＫＩが「０」のとき、ＴＳパケットのＰＩＤを検索キーとしてＰＩＤ検索テーブルＴ０を検索し、検索の結果得られた位置指定値Ｋｐに対応する暗号鍵を鍵テーブルＴｋｅｙから取得し、当該暗号鍵を用いて当該受信装置２１が属する同報グループ宛の同報通信を復号する。また復号部３４は、セクションヘッダのＣＫＩが「１」のとき、セクションヘッダに記入されたＭＡＣアドレスを検索キーとしてＭＡＣアドレス検索テーブルＴ１を検索し、検索の結果得られた位置指定値Ｋｐに対応する暗号鍵を鍵テーブルＴｋｅｙから取得し、当該暗号鍵を用いて当該受信装置２１宛の個別通信を復号する。

【０００９】以上の構成によれば、暗号鍵の実体を記憶した鍵テーブルＴｋｅｙと、当該鍵テーブルＴｋｅｙ内の各暗号鍵と検索キーとの対応関係を記述した同報通信用のＰＩＤ検索テーブルＴ０及び個別通信用のＭＡＣアドレス検索テーブルＴ１を鍵検索部３７に設け、ＰＩＤ又はＭＡＣアドレスを検索キーとしてＰＩＤ検索テーブルＴ０又はＭＡＣアドレス検索テーブルＴ１を検索し、当該検索キーに対応する位置指定値Ｋｐに基づいて鍵テーブルＴｋｅｙから暗号鍵を取得するようにしたことにより、ＰＩＤ検索テーブル及びＭＡＣアドレス検索テーブルそれぞれに鍵フィールドを設ける場合に比べ、鍵検索部３７の回路規模を削減することができる。

【０００９】例えばＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式の暗号化方式では、一般に４８～１２８ビット長程度の暗号鍵が用いられる。これに対して、衛星データ伝送システム１において１６個の暗号鍵を用いるとした場合、この全１６個の暗号鍵を指定するための位置指定値Ｋｐは４ビット長あれば良く、レコード内にフィールドとして直接鍵データを持つ場合に比べて検索テーブルのデータ量は格段に小さいものとなる。このため、２つの鍵テーブルを用いる場合にくらべ、１つの鍵テーブルと２つの検索テーブルを用いた方が、回路規模を削減することができる。

【０００９】また、検索テーブルを用いることにより、各鍵テーブル及び各検索テーブルのレコード数を独立かつ自由に決定することができ、これにより衛星データ送信システム１のシステム設計に高い自由度を与えることができる。

【０００９】例えば、検索テーブルを用いないとすると、複数のＭＡＣアドレスに対して同一の暗号鍵を割り当てる場合でも、鍵テーブルにはＭＡＣアドレスの個数と同じ数だけのフィールドを設ける必要がある。このフィールドには同一の暗号鍵を持つものが含まれる。これに対して検索テーブルを用いれば、鍵テーブルには暗号鍵の個数だけフィールドを設ければよい。

【０００９】さらに、各検索テーブルのデータ構造は独立して決定し得るため、ＰＩＤとＭＡＣアドレスのような異なるビット長の検索キーを併用することが容易になり、また検索テーブルの修正も容易になる。

【００００】（６）他の実施の形態
なお上述の実施の形態においては、衛星データ伝送システムに本発明を適用する場合について述べたが、本発明はこれに限らず、これ以外のデータ伝送システム、例えばケーブルインターネット等に適用しても良い。
【００００】また上述の実施の形態においては、同報通信と個別通信とを切り換えてデータ伝送する衛星データ伝送システムにおいて、２個の検索テーブルを使い分けて暗号鍵を検索するようにしたが、本発明はこれに限らず、通信方式の種類に応じて、３個以上の検索テーブルを使い分けて暗号鍵を検索するようにしたり、１個の検索テーブルを用いて暗号鍵を検索するようにしてもよい。
【００００】さらに上述の実施の形態においては、同報通信と個別通信とを切り換えてデータ伝送を行う衛星データ伝送システムにおいて、２個の検索テーブルと１個の鍵テーブルを設け、２個の検索テーブルのいずれか一方を用いて暗号鍵を検索するようにしたが、本発明はこれに限らず、単一の通信方法で２種類の暗号鍵系列を切り換えて暗号化を行う衛星データ伝送システムにおいて、１個の検索テーブルと２個の鍵テーブルを設け、当該２個の鍵テーブルのいずれか一方を用いて暗号鍵を検索するようにしてもよい。
【００００】図７はこの場合の鍵検索装置３７の構成例を示し、１個の検索テーブルＴ０と、２個の鍵テーブルＴｋｅｙ０及び鍵テーブルＴｋｅｙ１とを有しているとともに、当該鍵テーブルＴｋｅｙ０及びＴｋｅｙ１の一方を選択するセレクタ３７Ｂを有している。
【００００】検索テーブルＴ０は上述の実施の形態のＰＩＤ検索テーブルＴ０（図４）と同様のデータ構成を有している。また鍵テーブルＴｋｅｙ０も、上述の実施の形態の鍵テーブルＴｋｅｙ（図４）と同様に、Ｅｖｅｎ期間の鍵テーブルＴｋｅｙＥとＯｄｄ期間のＴｋｅｙＯとを有している。これに対して鍵テーブルＴｋｅｙ１はＥｖｅｎ期間とＯｄｄ期間の区別がなく、さらに暗号鍵のビット長が鍵テーブルＴｋｅｙ０とは異なる。
【００００】送信側システム２の送信処理装置１３（図１）は、制御装置１０の制御に応じて鍵テーブルＴｋｅｙ０又はＴｋｅｙ１のどちらか一方を選択し、送信先の同報グループのＰＩＤに対応した暗号鍵を用いてデータを暗号化した後送信する。
【００００】このとき送信処理装置１３は、セクションヘッダ内に設けたＫＴＳ（ＫｅｙＴａｂｌｅ　Ｓｅｌｅｃｔｉｏｎ）の値を、鍵テーブルＴｋｅｙ０を使用した場合は「０」に、鍵テーブルＴｋｅｙ１を使用した場合は「１」とする。このＫＴＳは、上述の実施の形態のＣＫＩとは異なる場所に設けることが望ましい。例えば図６に示すように、セクションヘッダ６バイト目の２番目のビット（図６の２行めの第２番目のバイトのＤ６）をＫＴＳと定めれば良い。
【００００】受信装置２１の復号部３４（図２）は鍵検索部３７に対して問い合わせを行い、ＫＴＳが「０」の場合、ＰＩＤに対応する暗号鍵を鍵テーブルＴｋｅｙ０から検索し、ＫＴＳが「１」で個別通信の場合、ＰＩＤに対応する暗号鍵を鍵テーブルＴｋｅｙ１から検索する。
【００００】すなわち鍵検索部３７のセレクタ３７Ｂ（図７）は、ＫＴＳが「０」のとき鍵テーブルＴｋｅｙ０を選択する。そして鍵検索部３７はＴＳパケットのＰＩＤを検索キーとして検索テーブルＴ０を検索し、ＰＩＤの値が合致するレコードに記録された位置指定値Ｋｐが示す暗号鍵を鍵テーブルＴｋｅｙ０から読み出して復号部３４に供給する。また鍵検索部３７のセレクタ３７Ｂは、ＫＴＳが「１」のとき鍵テーブルＴｋｅｙ１を選択する。そして鍵検索部３７はＰＩＤを検索キーとして検索テーブルＴ０を検索し、ＰＩＤの値が合致するレコードに記録された位置指定値Ｋｐが示す暗号鍵を鍵テーブルＴｋｅｙ１から読み出して復号部３４に供給する。
【００００】そして復号部３４は、かくして得た暗号鍵を用い、セクションのペイロードに配置されたＩＰパケットを復号する。
【００００】次に、この場合の復号処理手順を図８のフローチャートを用いて説明する。
【００００】復号部３４はＲＴ２で処理を開始し、ステップＳＰ２１においてＴＳパケットのＰＩＤをレジスタＰＲに代入し、次のステップＳＰ２２に進む。
【００００】ステップＳＰ２２において復号部３４は、セクションヘッダにおけるＰＳＣの下位ビットの値を参照し、当該セクションのペイロードに配置されたＩＰパケットが暗号化されているか否かを判断する。ステップＳＰ２２において否定結果が得られた場合、このことは下位ビットが「０」であり、当該セクションのペイロードに配置されたＩＰパケットが暗号化されていないことを表しており、復号部３４はステップＳＰ３１へ進み、暗号解除処理を行わずにセクションを後段のチェッカ３５に送出し処理を終了する。
【００００】これに対してステップＳＰ２２において肯定結果が得られた場合、このことはＰＳＣの下位ビットが「１」であり、当該セクションのペイロードに配置されたＩＰパケットが暗号化されていることを表しており、復号部３４はステップＳＰ２３に進む。
【００００】ステップＳＰ２３において、復号部３４は鍵検索部３７に対して問い合わせを行い、レジスタＰＲに記憶されているＰＩＤの値を検索キーとして検索テーブルＴ０を検索する。鍵検索部３７における検索テーブルＴ０の検索は、当該検索テーブルＴ０の先頭レコードから順に、ＰＩＤフィールド及び位置指定値フィールド双方のＶａｌｉｄビットがともに「１」なレコードに対してＰＩＤが合致するまで行われる。
【００００】そして復号部３４は、検索テーブルＴ０内

にＰＩＤが合致するレコードが存在しなかった場合、ステップＳＰ３０に移って当該セクションを破棄した後、ステップＳＰ３１に移って当該セクションに対する処理を終了する。

【００００】これに対して復号部３４は、検索テーブルＴ０内にＰＩＤが合致するレコードが存在した場合、ステップＳＰ２４に移って当該合致したレコードの位置指定値Ｋｐ［０］［ｙ］をレジスタＫｐに代入し、ステップＳＰ２５に移る。

【００００】ステップＳＰ２５において復号部３４は、セクションヘッダにおけるＫＴＳの値に基づいて、鍵テーブルＴｋｅｙ０又はＴｋｅｙ１のどちらを用いて暗号鍵を検索すべきかを判断する。ステップＳＰ２５において肯定結果が得られた場合、このことはＫＴＳが「１」であり、鍵テーブルＴｋｅｙ１を用いて暗号鍵を検索すべきことを表しており、復号部３４はステップＳＰ２６へ進む。

【００００】ステップＳＰ２６において復号部３４は、鍵テーブルＴｋｅｙ１から、レジスタＫｐの値に対応するＫｅｙ［Ｋｐ］を取り出してレジスタＫｅｙに代入するとともに、当該Ｋｅｙ［Ｋｐ］についてのＶａｌｉｄビットをレジスタＶａｌｉｄに代入し、次のステップＳＰ２７に移る。

【００００】これに対してステップＳＰ２５において否定結果が得られた場合、このことはＫＴＳが「０」であり、鍵テーブルＴｋｅｙ０を用いて暗号鍵を検索すべきことを表しており、復号部３４はステップＳＰ２８へ進む。

【００００】ステップＳＰ２８において復号部３４は、ＰＳＣの上位ビットをレジスタＥＯに代入する。そして復号部３４はレジスタＥＯの値が「０」のとき、Ｅｖｅｎ期間の鍵テーブルＴｋｅｙＥからレジスタＫｐの値に対応するＥｖｅｎ期間の鍵ＫｅｙＥ［Ｋｐ］を取り出してレジスタＫｅｙに代入するとともに、当該ＫｅｙＥ［Ｋｐ］についてのＶａｌｉｄビットをレジスタＶａｌｉｄに代入するのに対し、レジスタＥＯの値が「１」のとき、Ｏｄｄ期間の鍵テーブルＴｋｅｙＯからレジスタＫｐの値に対応するＯｄｄ期間の鍵ＫｅｙＯ［Ｋｐ］を取り出してレジスタＫｅｙに代入するとともに、当該ＫｅｙＯ［Ｋｐ］についてのＶａｌｉｄビットをレジスタＶａｌｉｄに代入し、ステップＳＰ２７に移る。

【００００】ステップＳＰ２７において復号部３４は、レジスタＶａｌｉｄの値に基づいて暗号鍵の有効／無効を判断する。ステップＳＰ２７において否定結果が得られた場合、このことはＰＩＤに対応する暗号鍵が存在するにもかかわらず、当該暗号鍵が無効状態にあることを表しており、復号部３４はステップＳＰ３０に移って当該セクションを破棄した後、ステップＳＰ３１に移って当該セクションに対する処理を終了する。

【００００】これに対してステップＳＰ２７において肯定結果が得られた場合、このことはＰＩＤに対応する暗号鍵が存在し、なおかつ当該暗号鍵が有効状態にあることを表しており、復号部３４は次のステップＳＰ２９に移る。

【００００】ステップＳＰ２９において復号部３４は、レジスタＫｅｙから鍵データを取り出し、当該鍵データを用いてセクションのペイロードを復号し、ステップＳＰ３１に移って処理を終了する。

【００００】かくして復号部３４は、検索テーブルＴ０と、２つの鍵テーブルＴｋｅｙ０及び鍵テーブルＴｋｅｙ１とを用いて、２種類の異なる暗号鍵系列に対応した復号処理を行う。

【００００】以上の構成によれば、検索テーブルＴ０と、複数の鍵テーブルとを用いて暗号鍵を検索するようにしたことにより、複数の暗号鍵系列を使い分けて暗号化し得るとともに、それぞれの暗号鍵系列における暗号鍵のビット長を自在に設定でき、衛星データ送信システム１のシステム設計に高い自由度を与えることができる。

【００００】さらに本発明は、複数の通信方式及び複数の暗号鍵系列をそれぞれ選択して使用するようなデータ伝送システムに適用することもできる。この場合、通信方式の種類に応じた個数の検索テーブル及び暗号鍵系列の種類に応じた個数の鍵テーブルを用意するとともに、選択使用した検索テーブル及び鍵テーブルをそれぞれ指定し得るビット長の選択符号（例えば上述したＣＫＩ及びＫＴＳ）をセクションヘッダ内に設ければよい。この場合でも検索テーブル及び鍵テーブルの個数はそれぞれ独立して設定でき、システム設計に高い自由度を与えることができる。

【００００】

【発明の効果】上述のように本発明によれば、複数の暗号鍵を記憶した鍵テーブルと、複数の検索キーと鍵テーブルにおける複数の暗号鍵との対応関係を記憶した検索テーブルとを設け、当該検索テーブルを検索キーで検索して鍵テーブルから暗号鍵を取得するようにしたことにより、簡易な構成で、様々な通信方法や暗号化方法に対応し得る情報伝送システムを実現できる。

【図面の簡単な説明】

【図１】本発明による衛星データ伝送システムの全体構成を示すブロック図である。

【図２】受信装置の回路構成を示すブロック図である。

【図３】セクションヘッダの構成を示す略線図である。

【図４】鍵検索部の構成を示す略線図である。

【図５】復号処理を示すフローチャートである。

【図６】他の実施の形態のセクションヘッダの構成を示す略線図である。

【図７】他の実施の形態の鍵検索部の構成を示す略線図である。

【図８】他の実施の形態の復号処理を示すフローチャー

トである。

【符号の説明】

１……衛星データ伝送システム、２……送信側システム、３……衛星、４……受信側システム、５……インターネット、１０……制御装置、１１……回線接続装置、１２……データサーバ、１３……送信処理装置、１４……ローカルネットワーク、１５……送信アンテナ、２０……受信アンテナ２０、２１……受信装置、２２……情報処理装置、２３……回線接続装置、２４……ローカルネットワーク、３０……ＣＰＵ、３１……フロントエンド部、３２……デマルチプレクサ、３３……受信フィルタ、３４……復号部、３５……チェッカ、３６……バッファ３７……鍵検索装置、……インターフェース部、３９……バス３９。

【図１】

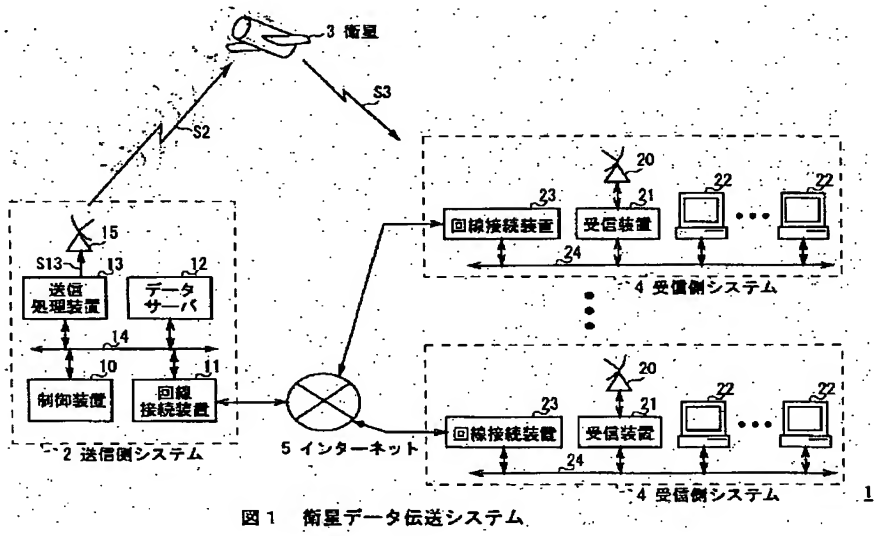


図１　衛星データ伝送システム

【図２】

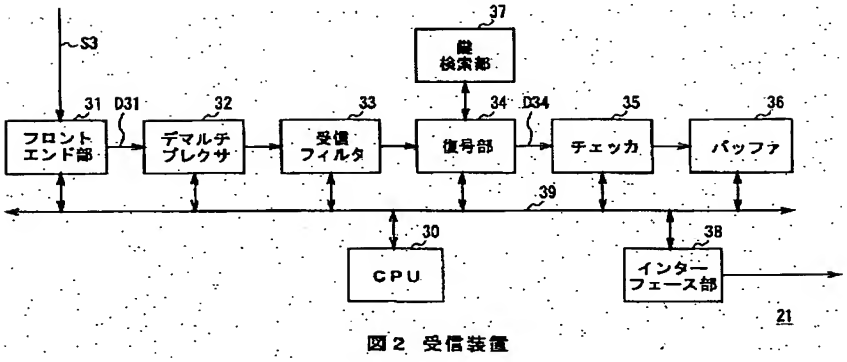


図２　受信装置

【図３】

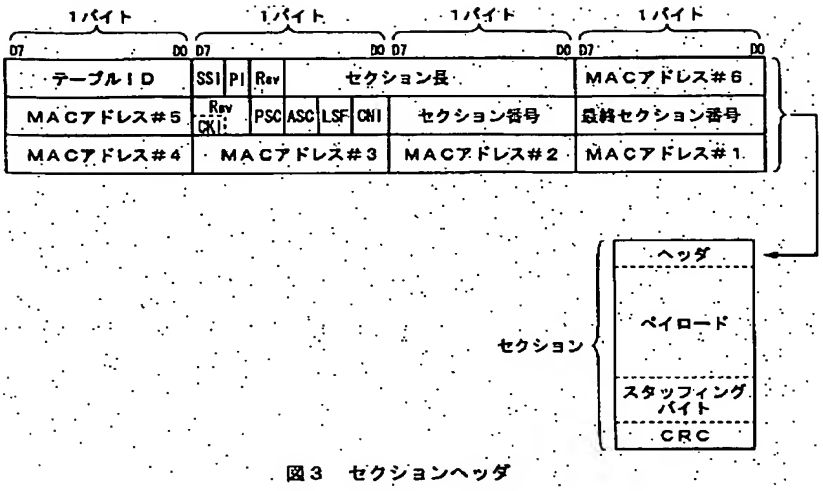


図３　セクションヘッダ

【図４】

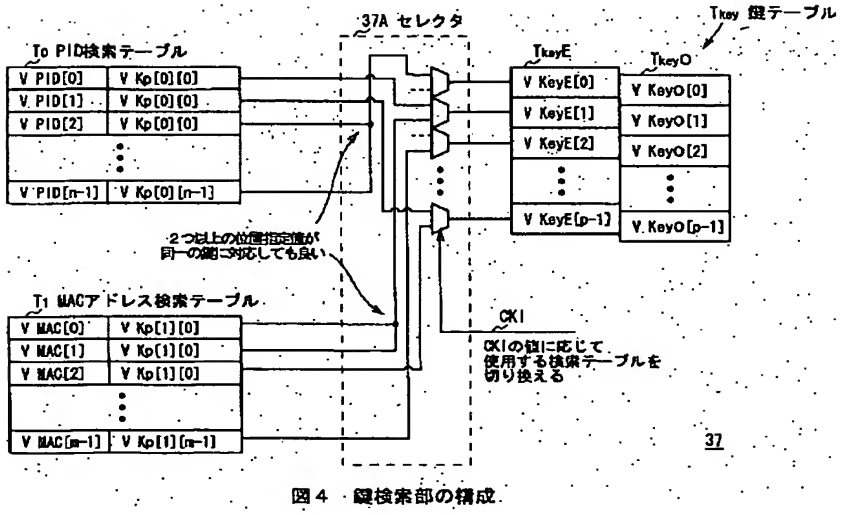


図４　鍵検索部の構成

【図５】

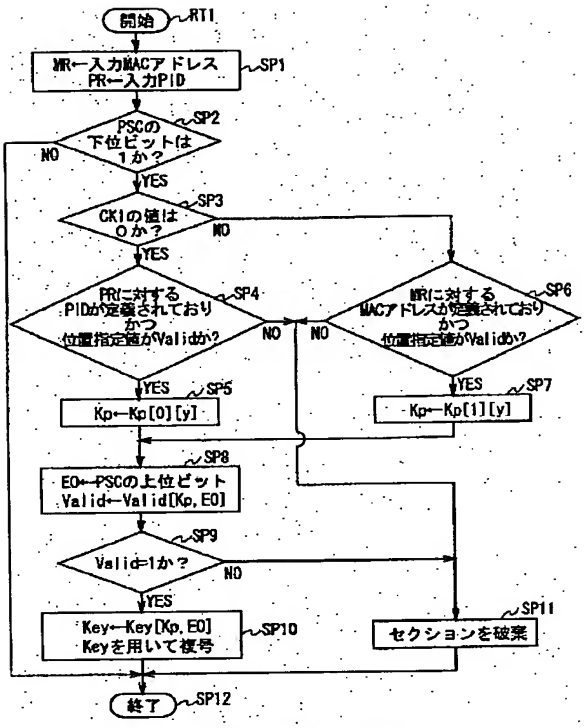


図５　復号処理手順

【図８】

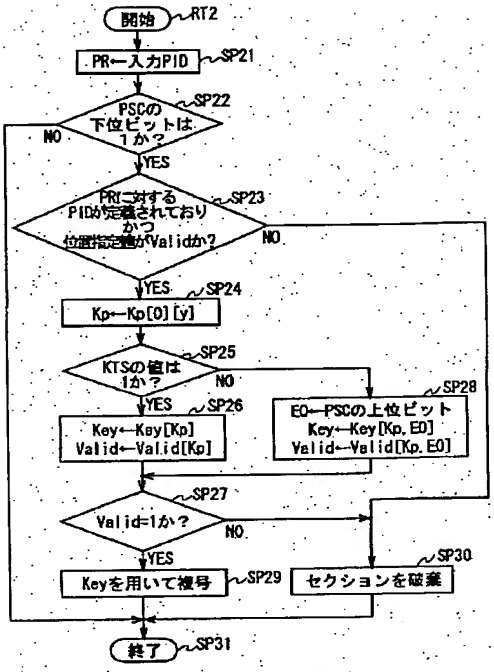


図８　他の実施の形態の復号処理

【図６】

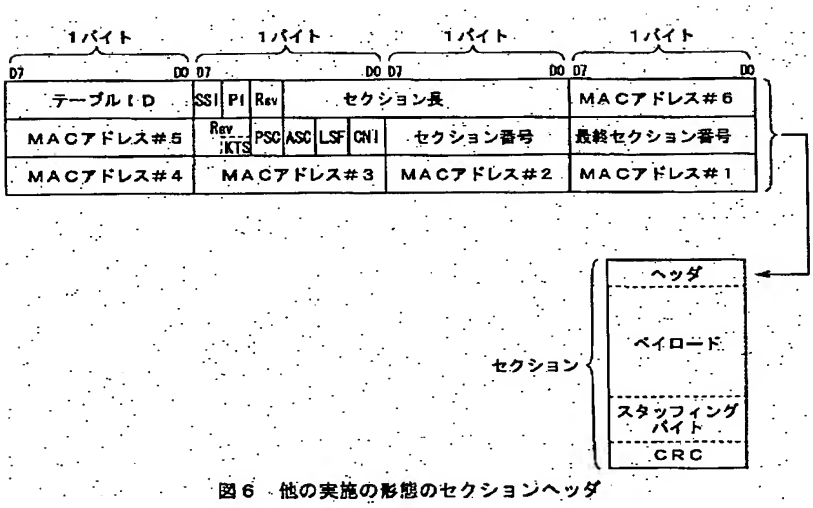


図６　他の実施の形態のセクションヘッダ

【図７】

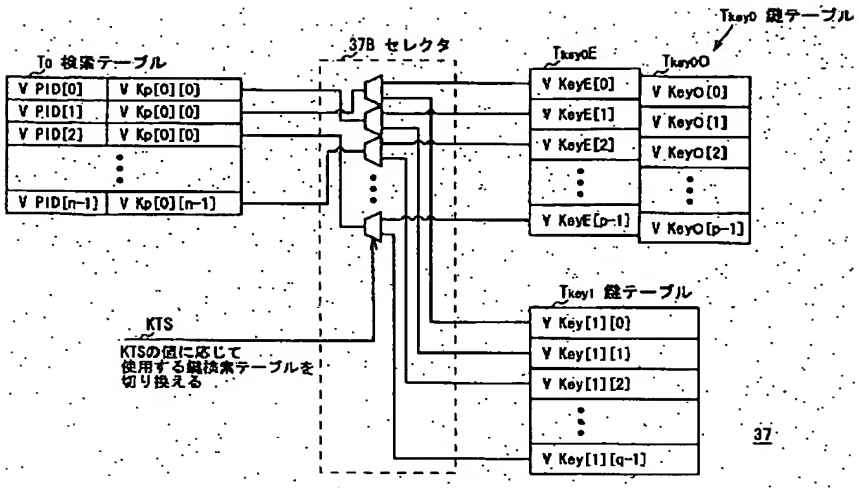


図７　他の実施の形態の鍵検索部の構成